

PAT-NO: JP411102345A
DOCUMENT- IDENTIFIER: JP 11102345 A
TITLE: METHOD AND SYSTEM FOR AUTHENTICATED DATA BASE
MANAGEMENT
PUBN-DATE: April 13, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
FUKUDA, TETSUYA	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC CORP	N/A

APPL-NO: JP09263493
APPL-DATE: September 29, 1997
INT-CL (IPC): G06F015/00 , G06F017/30

ABSTRACT:

PROBLEM TO BE SOLVED: To improve maintainance of an authenticated data base by constituting the authenticated data base with authenticated data of all users in all authentication management areas.

SOLUTION: The authenticated data base 1 consists of N records 2, which each consist of a user name field where a user name as a user identifier is written, a password field where a password as a password code is written, and an area field. One record is prepared for each user and user names set uniquely by the users are written in the user name files of the respective records. When a user accesses one of the authentication management areas, a user who has succeeded in authentication by accessing the authentication management area before this access is retrieved preferentially from the

authentication data base and matched against the current user to perform authentication.

COPYRIGHT: (C) 1999, JPO

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-102345

(43)公開日 平成11年(1999) 4月13日

(51)Int.Cl.⁶

G 0 6 F 15/00
17/30

識別記号

3 3 0

F I

G 0 6 F 15/00
15/40
15/403

3 3 0 B
3 2 0 B
3 4 0 A
3 4 0 B

審査請求 有 請求項の数8 OL (全 6 頁)

(21)出願番号

特願平9-263493

(22)出願日

平成9年(1997) 9月29日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 福田 哲也

東京都港区芝五丁目7番1号 日本電気株
式会社内

(74)代理人 弁理士 山川 政樹

(54)【発明の名称】 認証データベース管理方法および認証データベース管理システム

(57)【要約】

【課題】 ユーザ数が多くても認証時間を短くすることができ、また認証管理エリアが頻繁に変更されるようなことがあっても容易に保守を実施することができるようにする。

【解決手段】 各認証エリアに、複数のレコードによって構成され、各レコードは利用者毎に一意に付けられた利用者識別子が書き込まれたフィールドと、暗証符号の書き込まれたフィールドと、所定の初期値が予め書き込まれたエリアフィールドとによって構成された認証データベースを備える。

#1	ユーザ名 フィールド	パスワード フィールド	エリア フィールド	2
#2	taro	ABCDwxyz	0	
	⋮	⋮	⋮	1
#N	jiro	efghNOP	0	

【特許請求の範囲】

【請求項1】 複数の認証管理エリアに分割されるとともに、各認証管理エリアには全利用者に関する認証データベースが設置され、認証管理エリア毎に利用者の認証を実施するネットワークにおいて、利用者が前記認証管理エリアのうちの認証管理エリアに対してアクセスすると、このアクセス以前に前記一の認証管理エリアにアクセスして認証に成功した利用者を優先的に前記認証データベースの中から検索し、この検索された利用者と前記アクセスした利用者とを照合することによって認証を実施することを特徴とする認証データベース管理方法。

【請求項2】 請求項1において、利用者が前記認証管理エリアのうちの認証管理エリアに対してアクセスすると、このアクセスから所定時間以前までに前記一の認証管理エリアにアクセスして認証に成功した利用者を優先的に前記認証データベースの中から検索し、この検索された利用者と前記アクセスした利用者とを照合することによって認証を実施することを特徴とする認証データベース管理方法。

【請求項3】 複数の認証管理エリアに分割されるとともに、各認証管理エリアには全利用者に関する認証データベースが設置され、認証管理エリア毎に利用者の認証を実施するネットワークにおいて、前記各認証管理エリアは、利用者毎に一意に付けられた利用者識別子が書き込まれたフィールドと、暗証符号の書き込まれたフィールドと、認証の成功を示す符号の書き込まれるエリアフィールドとによって構成されたレコードを複数有する認証データベースと、この認証データベースを参照して利用者の認証を行い、利用者の認証に成功するとその利用者に係るレコードのエリアフィールドに認証の成功を示す符号を書き込み、また利用者から認証要求を受けるとエリアフィールドに認証の成功を示す符号の書き込まれているレコードを優先的に検索して認証を実施する認証サーバ手段と、この認証サーバ手段に接続され、利用者の認証要求を前記認証サーバ手段に送信するネットワークアクセスサーバ手段とを有することを特徴とする認証データベース管理システム。

【請求項4】 請求項3において、前記認証データベースを構成する各レコードは、認証に成功した日付の書き込まれる日付フィールドをさらに備え、前記認証サーバ手段は、前記認証データベースを参照して利用者の認証を行い、利用者の認証に成功するとその利用者のレコードのエリアフィールドに認証の成功を示す符号を書き込むとともに、その利用者に係るレコードの日付フィールドに認証を行った日付を書き込み、また

利用者から認証要求を受けるとエリアフィールドに認証の成功を示す符号の書き込まれているレコードを優先的に検索して認証を実施する手段であることを特徴とする認証データベース管理システム。

【請求項5】 請求項3において、前記エリアフィールドの代わりに、認証に成功した日付の書き込まれる日付フィールドが設けられていることを特徴とする認証データベース管理システム。

【請求項6】 請求項4において、前記認証サーバ手段は、前記日付フィールドの日付から所定の時間が経過するとエリアフィールドおよび日付フィールドの内容を、それぞれ所定の初期値に書き直す手段であることを特徴とする認証データベース管理システム。

【請求項7】 請求項3において、前記認証サーバ手段は、前記認証データベースに新たにレコードが追加されると、この追加されたレコードの利用者識別子フィールドに利用者により一意に付けられた利用者識別子を書き込み、暗証符号フィールドに所定の暗証符号を書き込み、エリアフィールドに所定の初期値を書き込む手段であることを特徴とする認証データベース管理システム。

【請求項8】 請求項4において、前記認証サーバ手段は、前記認証データベースに新たにレコードが追加されると、この追加されたレコードの利用者識別子フィールドに利用者により一意に付けられた利用者識別子を書き込み、暗証符号フィールドに所定の暗証符号を書き込み、日付フィールドに所定の初期値を書き込む手段であることを特徴とする認証データベース管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを複数の認証管理エリアに分割し、これら各認証管理エリア毎に認証サーバを設置して認証データベースを管理する方法およびシステムに関するものである。

【0002】

【従来の技術】一般的に、電話網等を介してパソコン通信やインターネット等のネットワークに接続する場合、利用者はパソコン通信会社やインターネットプロバイダ等によって提供された各地のアクセスポイントに接続し、このアクセスポイントを介して通信を行っている。

【0003】その際、ネットワークの正規のユーザであるか否かを確認するため、認証サーバは各利用者（以下、ユーザという）に対してユーザ名と一緒にパスワードの入力を要求する。そして、この入力されたユーザ名等をネットワーク内に予め設定されている認証データベースと照合し、両者が一致するとそのユーザの接続を許可する。

【0004】ところが、このようなパソコン通信等にお

いては、全国規模で事業を展開しているため、ユーザ数は多いところで数百万という規模に達するところもあり、アクセス時におけるユーザの認証に時間がかかり、この認証時間をいかにして短縮するかが従来より問題となっていた。

【0005】ここで、一般的なパソコン通信等におけるネットワークにおけるユーザの認証について図を用いて説明する。図6は、一般的なパソコン通信等のネットワークを模式的に表した説明図である。同図に示すように、ネットワーク全体は、5個の認証管理エリア10、20、30、40、50に分割されており、各認証管理エリアには認証サーバ11、21、31、41、51が設置されている。

【0006】そして、各認証サーバには、ルータとして機能するネットワークアクセスサーバ12、22、32、42、52がそれぞれ複数接続され、各ユーザはこれらネットワークアクセスサーバを介して認証サーバに接続される。なお、認証サーバおよびネットワークアクセスサーバは、何れもソフトウェア的に実現されることもあればハードウェア的に実現されることもある。

【0007】さて、図6に示すネットワークを、仮に全国規模のパソコン通信網に適用してみると、各認証管理エリアは関東、東北、近畿等の地方がそれぞれ対応し、これら各地方には1個ずつ認証サーバが設置される。そして、これら認証サーバに接続された複数のネットワークアクセスサーバは、各地方における市町村、例えば東京、三鷹、仙台、大阪等にそれぞれ設置されたアクセスポイントに対応する。

【0008】したがって、ユーザ13の住所を三鷹市とすれば、ユーザ13は最寄りのアクセスポイントである三鷹市のネットワークアクセスサーバ12を介してネットワークにアクセスし、関東地方のユーザ認証を一手に引き受けている認証サーバ11に接続される。

【0009】また、当然のことではあるが、ユーザ13は三鷹市以外にあるその他のネットワークアクセスサーバを介してアクセスすることもでき、例えばネットワークアクセスサーバ22を介してアクセスしたのであれば、認証管理エリア20内の認証サーバ21によって認証が行われる。このように、従来においては、ネットワーク全体が複数の認証管理エリアに分割され、各認証管理エリア毎に認証サーバが用意されてユーザの認証が行われていた。

【0010】

【発明が解決しようとする課題】しかしながら、以上のような従来の認証管理方法およびシステムにおいては、何れの認証管理エリアからでもアクセスできるようにするため、各認証管理エリアに全ユーザに関するデータを備えた認証データベースが設置されていた。そのため、ユーザの増加に伴ってレコード数が膨大になり、認証時における検索時間がかかるという問題点があった。

【0011】また、このような問題点を解決するため、認証管理エリア毎にユーザを割り振って認証データベースを小型化する方法もあるが、このような方法においてはアクセスした認証管理エリアに設置された認証データベースに該当するユーザが登録されていない場合、その他の認証管理エリアの認証データベースを参照することになるため、やはり時間がかかるという問題点があった。

【0012】さらに、上記のように認証管理エリア毎にユーザを割り振った場合、認証管理エリア毎に登録されているユーザが異なるため、認証管理エリアの追加および削除等が生じるとその他の認証管理エリア内の認証データベースも変更しなければならず、保守性において問題があった。特に、このような認証管理エリアの変更が頻繁に生じるネットワークにおいては、認証データベースの保守が非常に煩雑なものであった。

【0013】本発明は、このような課題を解決するためのものであり、複数の認証管理エリアを有するネットワークにおいて、ユーザ数が多くても認証時間を短くすることができ、また認証管理エリアが頻繁に変更されるようなことがあっても容易に保守を実施することができる認証データベース管理方法および認証データベース管理システムを提供することを目的とする。

【0014】

【課題を解決するための手段】このような目的を達成するために、本発明に係る認証データベース管理方法は、利用者が前記認証管理エリアのうちの認証管理エリアに対してアクセスすると、このアクセス以前に上記一の認証管理エリアにアクセスして認証に成功した利用者を優先的に上記認証データベースの中から検索し、この検索された利用者と上記アクセスした利用者とを照合することによって認証を実施するものである。このように構成することにより本発明に係る認証データベース管理方法は、ユーザ数が多くなっても短時間で検索することができ、また認証データベースの保守が容易である。

【0015】また、本発明に係る認証データベース管理システムは、各認証管理エリアは、利用者毎に一意に付けられた利用者識別子が書き込まれたフィールドと、暗証符号の書き込まれたフィールドと、認証の成功を示す符号の書き込まれるエリアフィールドとによって構成されたレコードを複数有する認証データベースと、この認証データベースを参照して利用者の認証を行い、利用者の認証に成功するとその利用者に係るレコードのエリアフィールドに認証の成功を示す符号を書き込み、また利用者から認証要求を受けるとエリアフィールドに認証の成功を示す符号の書き込まれているレコードを優先的に検索して認証を実施する認証サーバ手段と、この認証サーバ手段に接続され、利用者の認証要求を上記認証サーバ手段に送信するネットワークアクセスサーバ手段とを有する。このように構成することにより本発明に係る認

証データベース管理システムは、ユーザ数が多くなっても短時間で検索することができ、また認証データベースの保守が容易である。

【0016】

【発明の実施の形態】次に、本発明の一つの実施の形態について図を用いて説明する。図1は本発明の一つの実施の形態を示す説明図である。同図に示すように、認証データベース1はN個のレコード2によって構成され、各レコード2は利用者識別子であるユーザ名の書き込まれたユーザ名フィールドと、暗証符号であるパスワード

の書き込まれたパスワードフィールドと、エリアフィールドとによって構成されている。
【0017】例えば、図1の#2のレコードには、ユーザとして「tarō」が書き込まれ、パスワードとして「ABCdWxyz」が書き込まれている。そして、エリアフィールドには値「0」が書き込まれている。同様に、#nのレコードにはユーザ「jirō」についてのデータが書き込まれている。

【0018】このように、1ユーザに対して1個のレコードが用意され、各レコードのユーザ名フィールドにはユーザ毎に一意に設定されたユーザ名が書き込まれ、パスワードフィールドにはアルファベットや数字等の任意の組み合わせで作られたパスワードが書き込まれる。そして、エリアフィールドには初期値として「0」が書き込まれ、1度アクセスされると「1」が書き込まれる。

【0019】ここで、認証データベースに新たにユーザを登録する際の手順について図を用いて説明する。図4は、認証データベースに新たにユーザを登録した様子を示す説明図である。同図に示すように、#N+1のレコードに新たにユーザ「hanako」を登録した場合、パスワードフィールドには任意に設定されたパスワードとして例えば「KLMS tu vW」が書き込まれる。そして、エリアフィールドには、初期値「0」が書き込まれる。

【0020】次に、認証の手順について図を用いて説明する。図5は、図1に係る認証データベースを図6に係る一般的なネットワークに用いたときの認証手順を示すフローチャートである。なお、以下においては図6のユーザ13が認証サーバ11にアクセスする手順を例にとりて説明するが、他の認証サーバ等についても同様に実施される。

【0021】まず、ステップ100において、ネットワークアクセスサーバ12を介してユーザ13からの認証要求が認証サーバ11に送信されると、認証サーバ11は認証を開始する。ステップ101において、既にこの認証サーバ11にアクセスしたことのあるユーザを優先的に検索するため、認証サーバ11は、認証データベース中のエリアフィールドの値が「1」であるレコードの検索を開始する。そして、該当するレコードがあればステップ102へ移行し、なければステップ105へ移行

する。

【0022】ステップ102において、認証データベース中に該当するレコードを検索することができたため、引き続いてパスワードの照合を行う。すなわち、認証サーバ11は、入力されたパスワードと検索されたレコードのパスワードとを照合し、互いに一致するか否かを確認する。そして、一致すればステップ103へ移行し、一致しなければステップ106へ移行する。

【0023】ステップ103において、認証サーバ11は、入力されたユーザ名およびパスワードが認証データベースに登録されているものと一致することを確認できたので、ネットワークアクセスサーバ12に対して認証の成功を通知する。その結果、ユーザ13は、ネットワークへの接続が許可されて通常の手順によってネットワークへのアクセスが実施される。ステップ104において、認証サーバ11は、アクセス済みを示す値「1」をエリアフィールドに書き込んで認証手続を終了する。

【0024】一方、ステップ105において、認証サーバ11は、エリアフィールドの値が「0」のレコードを検索する。そして、該当するレコードがあればステップ102へ移行し、上記同様にパスワードの照合等を行う。また、該当するレコードがなければステップ106へ移行する。

【0025】ステップ106において、パスワードが一致しなかったり、認証データベース内にアクセスしたユーザが登録されていなかったりしたため、認証アクセスサーバ11はネットワークアクセスサーバ12に対して認証の失敗を通知する。その結果、ユーザ13は、ネットワークへの接続を拒否される。

【0026】次に、本発明のその他の実施の形態について説明する。図2は、本発明のその他の実施の形態を示す説明図である。同図に示すように、図1の構成とよく似ているがエリアフィールドの代わりに日付フィールドが設けられている点が異なっている。

【0027】すなわち、認証の成功時に、認証を行った日付（年月日または時刻）を書き込むようにすれば、検索時に日付の書き込まれたレコードを優先的に検索することによって図1の場合と同様の効果を得ることができる。

【0028】また、図2の場合は、日付フィールドに書き込まれている日付を定期的に監視し、その日付から一定時間が経過すると日付フィールドを初期値に書き直すことにより、アクセス回数の少ないユーザの日付フィールドを初期化する。その結果、頻繁に認証管理エリア10内でアクセスするユーザを優先的に検索することができるようになり、図1の場合よりも認証時間をさらに短縮することができる。

【0029】さらに、図2の認証データベースを用いたときの認証手順は、図1の場合とはほぼ同様であるため、概ね図5のフローチャートに従う。ただし、ステップ1

04においてエリアフィールドに書き込む代わりに、日付フィールドに認証を行った日付を書き込む点が異なる。また、認証データベース11は、認証手続きとは独立して定期的に日付フィールドの日付を監視し、現在の時刻から遡って一定時間経過したものはその日付フィールドの値を所定の初期値、例えば「00.00.00」に書き直す。

【0030】図3は、本発明のさらにその他の実施の形態を示す説明図である。同図に示すように、これは図1の構成と図2の構成とを組み合わせたものであり、エリア

【0031】

【発明の効果】以上説明したように本発明は、認証データベースは全認証管理エリアにおける全てのユーザの認証データによって構成されているため、認証管理エリアが変更されてもそれ以前の認証データベースをそのまま

明は、認証管理エリア毎に全エリアにおけるユーザを登録した認証データベースが設置されているけれども、エリアフィールド等を利用して検索するレコードを限定することにより、検索を高速化させることができる。

【図面の簡単な説明】

【図1】 本発明の一つの実施の形態を示す説明図である。

【図2】 本発明のその他の実施の形態を示す説明図である。

【図3】 本発明のその他の実施の形態を示す説明図である。

【図4】 図1に係る認証データベースに、新たにユーザを登録した様子を示す説明図である。

【図5】 本発明に係る認証手順を示すフローチャートである。

【図6】 複数の認証管理エリアを有するネットワークを示す説明図である。

【符号の説明】

1…認証データベース、2…レコード、10、20、30、40、50…認証管理エリア、11、21、31、41、51…認証サーバ、12、22、32、42、52…ネットワークアクセスサーバ、13…ユーザ。

【図1】

#1	ユーザ名 フィールド	パスワード フィールド	エリア フィールド
#2	taro	ABCDwxyz	0
	⋮	⋮	⋮
#N	jiro	efghMNOP	0

【図2】

#1	ユーザ名 フィールド	パスワード フィールド	日付 フィールド
#2	taro	ABCDwxyz	00.00.00
	⋮	⋮	⋮
#N	jiro	efghMNOP	00.00.00

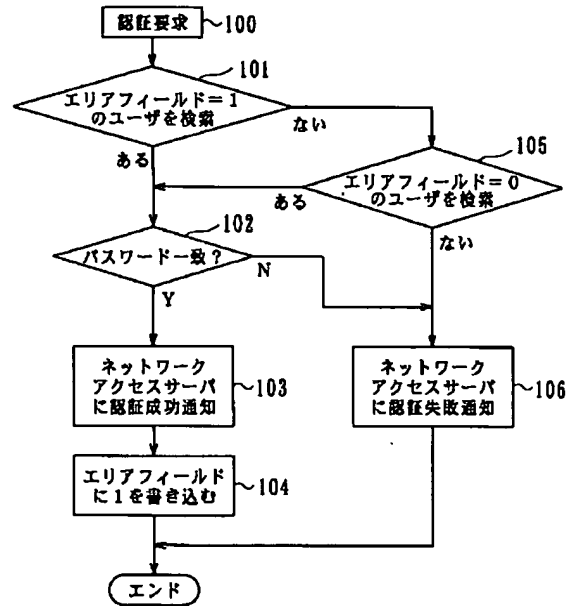
【図3】

#1	ユーザ名 フィールド	パスワード フィールド	エリア フィールド	日付 フィールド
#2	taro	ABCDwxyz	0	00.00.00
	⋮	⋮	⋮	⋮
#N	jiro	efghMNOP	0	00.00.00

【図4】

#1	ユーザ名 フィールド	パスワード フィールド	エリア フィールド
	⋮	⋮	⋮
#N	jiro	efghMNOP	1
#N+1	hanako	KLmstuvW	0

【図5】



【図6】

